

05/03/99 1c654 U.S. PTO

A

1c549 U.S. PTO  
09/30/035  
05/03/99

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventorship ..... Vanzini et al.  
Applicant ..... Microsoft Corporation  
Attorney's Docket No. .... MS1-254US  
Title: PCMCIA-compliant Smart Card Secured Memory Assembly For Porting User Profiles and Documents

TRANSMITTAL LETTER AND CERTIFICATE OF MAILING

To: Commissioner of Patents and Trademarks  
Washington, D.C. 20231  
From: Lewis C. Lee (509) 324-9256  
Lee & Hayes, PLLC  
W. 201 North River Drive, Suite 430  
Spokane, WA 99201

The following enumerated items accompany this transmittal letter and are being submitted for the matter identified in the above caption.

1. Transmittal Letter with Certificate of Mailing included.
2. PTO Return Postcard Receipt
3. New patent application (title page plus 27 pages, including claims 1- 38 & Abstract)
4. Executed Declaration
5. 4 sheets of formal drawings (Figs. 1- 5)
6. Assignment w/Recordation Cover Sheet

Large Entity Status ☒ Small Entity Status ☐

The Commissioner is hereby authorized to charge payment of fees or credit overpayments to Deposit Account No. 50-0463 in connection with any patent application filing fees under 37 CFR 1.16, and any processing fees under 37 CFR 1.17.

Date: May 3, 1999

By: L. C. Lee  
Lewis C. Lee  
Reg. No. 34,656

CERTIFICATE OF MAILING

I hereby certify that the items listed above as enclosed are being deposited with the U.S. Postal Service as either first class mail, or Express Mail if the blank for Express Mail No. is completed below, in an envelope addressed to The Commissioner of Patents and Trademarks, Washington, D.C. 20231, on the below-indicated date. Any Express Mail No. has also been marked on the listed items.

Express Mail No. (if applicable)

EL209423130

Date: 5/3/99

By: Dana L. Calhoun  
Dana L. Calhoun

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

**PCMCIA-compliant Smart Card Secured Memory  
Assembly For Porting User Profiles and Documents**

Inventor(s):

Giorgio J. Vanzini

Gregory Burns

## **TECHNICAL FIELD**

This invention relates to systems and methods for transporting user profiles and data files from one computer to another. More particularly, this invention relates to a portable profile carrier that enables a user to securely store and transport a user profile and personal data files, while allowing the user to access the profile and data files during log on processes at a standalone or networked computer so that the computer retains the same 'look and feel' of the user's desktop and setup.

## **BACKGROUND**

Profiles are used by operating systems to configure operating characteristics of a computer (e.g., user interface schema, favorites lists, etc.) according to user-supplied preferences and provide storage for the user's personal data files (e.g., files on the desktop or in the user's "my documents" folder. Windows NT operating systems from Microsoft Corporation supports two types of profiles: local profiles and roaming profiles. A local profile is stored and loaded from a fixed location on the local computer. The profile remains at the computer, and is not portable to another computer. Thus, if the user logs onto another computer, a new profile is created for that user from a default profile. As a result, the user ends up with different profiles on each machine that he/she logs onto and hence, each machine looks and feels differently.

A roaming profile travels with the user in a networked environment and is made available to the user regardless of which machine the user logs onto. Fig. 1 shows a client-server architecture 20 that implements conventional roaming profiles. The architecture 20 includes a server 22 connected to serve a client 24

over a network 26. The server 22 has an operating system 28 and a profile store 30 that holds various user profiles. The profiles are associated with the users via a passcode. The client 24 runs an operating system 32.

When the user logs onto the client 24, the user is initially prompted for a user name, domain name, and password. The domain name is used to identify the server 22 and the user name is used to locate a corresponding user profile from the profile store 30. If a profile exists (i.e. the user name is known to the server), the password is used in a challenge response exchange with the server to verify the identity of the user. If the user provided the correct password for the given user name the user's profile is downloaded from the server 22 to the client 24 and used to configure the client according to the user's preferences.

If additional security is warranted, the architecture may further include smart card tokens. The user is assigned a personal smart card and inserts the smart card into a card reader at the client. In this case the user name, domain name, and password is stored on the smart card. Instead of the user entering this information the user enters a passcode that unlocks the card and makes the information available to the client which then performs the logon process as described above.

One drawback with the roaming architecture is that users have only limited control over their own profiles. A user cannot, for instance, establish a roaming profile without the assistance of a network administrator. The administrator must assign a roaming profile pathname in the user's account on the domain server. The user then has the option to indicate on each machine whether to use a roaming profile or a local profile.

Another drawback with roaming profiles is that the architecture restricts roaming to clients connected to the network 26 with access to the domain server

1 and the profile server 22. The architecture does not allow a user to access his/her  
2 profile on a home computer or other standalone computer that is not network  
3 attached.

4 Accordingly, there is a need for a portable device that securely transports a  
5 user's profile and related documents (My Documents) to various machines,  
6 regardless of whether the machines are connected or standalone. The inventors  
7 have developed such a device.

## 8 9 **SUMMARY**

10 This invention concerns a portable profile carrier that stores and securely  
11 transports a user's profile and personal user data files from one computer to the  
12 next.

13 The profile carrier is a two-component assembly comprising a storage card  
14 (e.g., smart card) and a card reader. The reader is physically constructed in a form  
15 factor of a PCMCIA card and has a slot to receive the storage card. The reader has  
16 a card interface and controller to facilitate data communication with the storage  
17 card.

18 According to an aspect of this invention, the reader is equipped with data  
19 memory (e.g., flash memory) to store the user profile and data files. The storage  
20 card protects access to the data memory. The composite profile carrier alternately  
21 enables access to the user profile on the flash memory when the card is present  
22 and the user is authenticated, while disabling access when the card is removed or  
23 the user is not authenticated within a certain time period.

24 In one implementation, the storage card is implemented as a smart card  
25 having processing capabilities. The card reader is implemented as a smart card

1 reader. The profile assembly is assigned a pair of public and private keys, with the  
2 public key being stored on the smart card reader and the private key being kept on  
3 the smart card. The smart card also stores a passcode that is unique to the user.

4 To access the contents in the flash memory, the user assembles the card  
5 reader and smart card and inserts the assembled carrier into a PCMCIA device  
6 reader at the computer. The user is prompted to enter a passcode and the smart  
7 card authenticates the user by comparing the user-supplied passcode to the stored  
8 passcode. Assuming that the user is legitimate, the smart card then authenticates  
9 the smart card reader by determining whether the public key is complementary  
10 with the private key. If it is, access to the user profile and data files on the flash  
11 memory is permitted.

#### 12 13 **BRIEF DESCRIPTION OF THE DRAWINGS**

14 Fig. 1 is a block diagram of a prior art client-server system that supports  
15 roaming profiles from one network client to another.

16 Fig. 2 is a block diagram of system having a portable profile carrier that  
17 securely transports user profiles and data files from computer to computer. The  
18 portable profile carrier, in conjunction with the computer operating system,  
19 enables authenticated access to the profiles and documents at a computer,  
20 regardless of whether the computer is standalone or networked.

21 Fig. 3 is a diagrammatic view of a composite profile carrier that includes a  
22 smart card reader and a smart card.

23 Fig. 4 is a block diagram of the system components, including the computer  
24 operating system, smart card, and smart card reader.

1 Fig. 5 is a flow diagram showing steps in a two-phase authentication  
2 process for accessing user profile and data files carried on the profile carrier.

3 The same numbers are used throughout the figures to reference like  
4 components and features.

## 5 6 **DETAILED DESCRIPTION**

7 This invention concerns a portable profile carrier for transporting a user  
8 profile from one computer to the next in order to configure each computer  
9 according to user preferences. The profile carrier is equipped with sufficient  
10 memory to hold data files as well as the user profile. In one implementation, the  
11 profile and data files are secured, in part, using cryptographic techniques.  
12 Accordingly, the following discussion assumes that the reader is familiar with  
13 cryptography. For a basic introduction of cryptography, the reader is directed to a  
14 text written by Bruce Schneier and entitled "Applied Cryptography: Protocols,  
15 Algorithms, and Source Code in C," published by John Wiley & Sons with  
16 copyright 1994 (second edition 1996).

### 17 18 **System**

19 Fig. 2 shows a computer system 50 having a computer 52 and a portable  
20 profile carrier 54. The computer 52 has an operating system 56 and a PCMCIA  
21 (Personal Computer Memory Card Interface Association) device reader 58 that is  
22 capable of reading PCMCIA cards, which are also referred to as PC cards. The  
23 computer may be configured as a general-purpose computer (e.g., desktop  
24 computer, laptop computer, personal digital assistant, etc.), an ATM (automated  
25 teller machine), a kiosk, an automated entry system, a set top box, and the like.

1 The machine 52 may be a standalone unit or networked to other computers (not  
2 shown).

3 The profile carrier 54 stores a user's profile in a secured medium that can  
4 be conveniently transported. The profile consists of user information that can be  
5 used to configure computer 52 according to selected preferences and schema of  
6 the user. The profile contains essentially all of the information that is useful or  
7 personal to the user. For instance, a profile might include a user's name, logon  
8 identity, access privileges, user interface preferences (i.e., background, layout,  
9 etc.), mouse control preferences (i.e., click speed, etc.), favorites lists, personal  
10 address book, the latest electronic mail (sorted according to user criteria) and so  
11 forth. One can also envision that application tokens or keys can be stored, and that  
12 will allow the user to access or use the applications for which he/she has tokens or  
13 keys.

14 The profile carrier 54 is an assembly of two components: a card reader 60  
15 and a storage card 62. At its most basic form, the storage card 62 has a memory to  
16 store a passcode associated with the user. Higher forms of the storage card can be  
17 implemented, such as an integrated circuit (IC) card that has both memory and  
18 processing capabilities. In particular, the storage card 62 can be implemented as a  
19 smart card equipped with private memory for storing private keys (or other user  
20 secrets) and processing capabilities, including rudimentary cryptographic  
21 functionality (e.g., encryption, decryption, signing, and authentication). Smart  
22 card technology enables utilization of private keys without exposing them to the  
23 external world.

24 The card reader 60 provides an interface to read and write data to the  
25 storage card 62. The card reader 60 is preferably implemented as a PCMCIA (but



could also be implemented via other means, e.g. via Universal Serial Bus, aka USB) smart card reader that is constructed in a form factor of a PCMCIA card so that it may be compatibly received by the PCMCIA device reader 58 at the computer 52. According to an aspect of this invention, the smart card reader 60 is equipped with data memory, such as flash memory, to hold the user's profile and other data files.

According to this architecture, the two-component profile carrier forms a smart card secured memory assembly that alternately enables access to the user profile on the reader-based flash memory when the smart card is present, while disabling access to the user profile when the smart card is removed. The smart card is associated with the user (e.g., via a passcode, like a ATM card) to ensure that only the legitimate user can access the smart card. In addition, the smart card reader 60 and smart card 62 are associated with one another (e.g., by sharing a public/private key pair) to securely link the legitimate user to the user profile and files stored in the flash memory of the smart card reader 60.

### **Portable Profile Carrier**

Fig. 3 shows the profile assembly 54 in more detail. The smart card reader 60 is sized according to a PCMCIA form factor and includes a PCMCIA compatible connector 64 to accommodate insertion into and communication with the PCMCIA device reader 58 at the computer 52. The smart card reader 60 defines a slot to receive the smart card 62, whereby the smart card 62 can be alternately inserted into the reader slot or removed from the reader slot. When inserted, contacts on the smart card align with an interface 66 in the smart card reader 60 to allow communication between the smart card and reader. The smart

1 card reader 60 also has a controller 68 coupled between the card interface 66 and  
2 connector 64 to facilitates data communication between the computer 52 and the  
3 smart card 62.

4 The smart card reader 60 described thus far is of conventional design.  
5 There are existing smart card readers with a PCMCIA form factor. Examples of  
6 such smart card readers for PCMCIA are made by SCM Microsystems.

7 Unlike conventional smart card readers, however, smart card reader 60 is  
8 equipped with additional data memory 70 to hold the user profile and user files.  
9 The data memory can be implemented as flash memory, on the order of currently  
10 up to 128 MB, to hold a substantial amount of user data. The data memory 70 is  
11 coupled to the controller 68 via a data bus (not shown) to enable access to the data.

12 Fig. 4 shows functional components in the computer system 50. Computer  
13 52 includes operating system 56 and reader 58. The operating system 56 has a  
14 logon module 80 to facilitate the user logon process. For a Windows NT operating  
15 system from Microsoft Corporation, the logon module 80 would be a modified  
16 version of the dynamic link library "msgina.dll", a component used by the user  
17 logon facility "winlogon.exe".

18 The operating system 56 also has a smart card and flash memory driver 82.  
19 The composite driver 82 is capable of detecting whether the device inserted into  
20 the PCMCIA reader 58 is a "combo" device that includes both flash memory and a  
21 smart card. The modified logon module ("msgina.dll") is designed to recognize  
22 that a profile assembly 54 has been inserted into the PCMCIA reader 58 (or  
23 alternatively, has established a USB connection). For discussion purposes, the  
24 modified logon module for handling the profile assembly will be referred to as  
25

1 “picoauth.dll”. Logon procedures are described below under the heading  
2 “Portable Profile Operation”, with reference to Fig. 5.

3 With continuing reference to Fig. 4, the profile assembly 54 comprises the  
4 smart card reader 60 and smart card 62. The smart card reader 60 has connector  
5 64, card interface 66, controller 68, and flash memory 70. A multi-bit bus (not  
6 shown) connects the components. The flash memory 70 is partitioned into a  
7 public area 84 and a private area 86. A public key 90 is stored in the public area  
8 84 of the flash memory 70 and can be exported from the smart card reader 60.  
9 The public key 90 is from a public/private key pair assigned to the profile carrier,  
10 with the corresponding private key being kept on the smart card. A user profile 92  
11 and data files 94 are stored in the private area 86 of flash memory 70.

12 The detailed internal architecture of smart cards varies greatly between  
13 smart cards from different manufacturers. For purposes of this discussion, a very  
14 simplified view of a typical smart card is used. The smart card 72 has an interface  
15 100, a microcontroller or processor 102, and secured storage 104. The  
16 microcontroller 102 is preprogrammed to perform certain cryptographic functions  
17 and can read from and write to the secured storage 104. The microcontroller 102  
18 responds to commands sent via the interface 100 and can send data in response to  
19 those commands back to the interface.

20 In this simplified smart card 62, the secured storage 104 contains a  
21 passcode 106, a private key 108, and an encryption key 110. Before it will  
22 perform any cryptographic functions involving private key 108, the smart card 62  
23 is unlocked by a command sent in via the interface 100 that specifies a passcode  
24 matching the stored passcode 106. Once unlocked, the smart card can be  
25 instructed by other commands to perform cryptographic functions that involve the

1 use of the private key 108, without making the private key available outside of the  
2 smart card.

3 The programming of the microcontroller 102 is designed to avoid exposing  
4 the passcode 106 and the private key 108. Simply, there are no commands that  
5 can be issued to the microcontroller 102 via the interface 100 that will reveal the  
6 values of the passcode and the private key. In this manner, the smart card prevents  
7 a foreign application from ever inadvertently or intentionally mishandling the  
8 passcode and keys in a way that might cause them to be intercepted and  
9 compromised. In constructing smart cards, manufacturers take additional  
10 measures to ensure that the secured storage is inaccessible even when the smart  
11 card is disassembled and electronically probed.

### 12 13 **Portable Profile Operation**

14 The system described above enables a user to transport his/her profile and  
15 data files on a secured portable device from one computer to the next. The user  
16 can upload the user profile from the portable device to the computer and  
17 automatically configure the computer to his/her likes and preferences. In this  
18 manner, every computer "looks and feels" the same to the user, based on that  
19 user's settings and preferences.

20 The profile carrier is configured as a smart card secured flash memory  
21 assembly that alternately enables access to the user profile in flash memory when  
22 the smart card is present, while disabling access when the smart card is removed.  
23 No connection to a server for remote downloading of profiles is necessary, as the  
24 portable profile carrier contains all of the information needed by the computer for  
25 customized configuration.

1 To access the user profile, the user assembles the card reader 60 and smart  
2 card 62 by inserting the smart card 62 into the slot in the reader 60 to align the  
3 contacts with the card interface 66. The user then inserts the assembled carrier  
4 into the PCMCIA device reader 58 at the computer 52. Authorization to access  
5 the user profile is achieved through a two-phase authentication process. One  
6 phase involves user authentication in which the smart card 62 authenticates the  
7 user via a passcode challenge. The second phase concerns assembly  
8 authentication in which the smart card 62 authenticates the smart card reader 60 as  
9 carrying the profile of the user.

10 Fig. 5 shows steps in the two-phase authentication process that enables  
11 access to the user profile and data files. The steps are performed in a combination  
12 of hardware and software resident at the computer 52, smart card reader 60, and  
13 smart card 62. The method is also described with additional reference to the  
14 system illustrated in Fig. 4.

15 At step 150, the computer 52 monitors for insertion of a PCMCIA-  
16 compatible device in PCMCIA device reader 58. In one implementation, the  
17 logon "picoauth.dll" module 80 of operating system 56 continually monitors the  
18 PCMCIA device reader 58. When insertion is detected, the picoauth.dll module  
19 80 queries the device to determine whether it is a profile assembly having both  
20 flash memory and a smart card. Once the profile assembly is identified, the logon  
21 module 80 proceeds with the logon procedure.

22 At step 152, the computer operating system 56 prompts the user via a  
23 dialog box or other type window to enter a passcode, such as a PIN (Personal  
24 Identification Number). After the user enters the passcode, the smart card/flash  
25

The smart card microcontroller 102 compares the user-supplied passcode to the passcode 106 stored in secured storage 104 (step 156). If the two fail to match (i.e., the “no” branch from step 158), the microcontroller 102 rejects the entered passcode and returns a failure notice (step 160). Conversely, if the two match, the user is said to have been authenticated and the microcontroller 102 will now accept commands that involve cryptographic operations involving the private key 108 and the encryption key 110.

In this manner, the smart card is associated with a particular user through the passcode. Only the legitimate user is assumed to know the passcode and hence, only the legitimate user is able to unlock the smart card.

This passcode challenge completes the user authentication phase of the process. The assembly authentication phase is subsequently initiated to determine whether the flash memory device carries the data of the authenticated user. This phase employs public key cryptography to make this determination. As noted above, the composite profile assembly is assigned a pair of complementary public and private keys, with the public key 90 being stored in flash memory 70 on smart card reader 60 and the corresponding private key 108 being stored in the secured storage 104 of the smart card 62.

At step 164, the smart card/flash memory driver 82 reads the public key 90 from the public area 84 of flash memory 70 on the smart card reader 60. The driver 82 passes the public key 90 to the smart card 62 via the computer-based PCMCIA device reader 58 and smart card reader 60 (step 166). The smart card microcontroller 102 runs a process using the public key 90 and the private key 108

1 from secured storage 104 to determine whether the keys are complementary (step  
2 168). This step determines whether the smart card reader 60 and smart card 62 are  
3 associated with one another and form the user's profile carrier, thereby linking the  
4 legitimate user to the user profile and files stored in the flash memory of the  
5 profile carrier.

6 If the public key is not valid (i.e., the "no" branch from step 170), the  
7 microcontroller 102 rejects the entered public key and returns a failure notice  
8 indicating that the card reader does not correspond to the smart card (step 172).  
9 On the other hand, assuming the public key checks out (i.e., the "yes" branch from  
10 step 170), the smart card instructs the controller 68 on the smart card reader 60 to  
11 enable access to the user profile and data files in the private area 86 of the flash  
12 memory 70 (step 174). At this point, the computer is permitted to read the user  
13 profile and data files from the flash memory 70 and normal logon processes are  
14 continued using the profile data from the flash memory (step 176).

15 The computer configures the computer according to the user profile. The  
16 flash memory is also made available as a peripheral storage device for the  
17 computer. The operating system presents an icon or name in a file system user  
18 interface to inform the user that the memory is addressable and available.

19 After the user completes a session at this computer, the user can save any  
20 files or other data to the flash memory. The user is then free to remove the profile  
21 assembly from the computer and carry it to another computer. The user can then  
22 repeat the same operation described above to import his/her profile to the next  
23 computer.

24 The scheme described is secure if the computer 52 can be trusted to  
25 correctly pass the public key 90 to the smart card 62, and correctly pass the

1 accepts/reject response from the smart card 62 to the controller 68. To further  
 2 protect the private area 86 in the smart card reader 60, the contents of the private  
 3 area 86 can be encrypted (e.g. DES encryption) using a key that can only be  
 4 obtained from the smart card 62 after the smart card has been successfully  
 5 unlocked by the user providing the correct passcode. In this case, the computer 52  
 6 must send a command to the smart card 62 via the interface 100 to obtain the  
 7 encryption key 110, which it passes to the controller 68. The controller uses this  
 8 key to decrypt the user profile 92 and user documents 94 as the computer makes  
 9 requests to read this data. Similarly when this data is written back to the reader  
 10 60, the controller 68 uses the key to encrypt the data before writing it to the private  
 11 memory area 86. The smart card will only provide the encryption key if it has  
 12 been previously unlocked, meaning that a user provided the correct passcode.

### 13 14 **Storage Card Implementation**

15 The above processes assume that storage card 62 is an IC card or smart card  
 16 with processing capabilities in addition to memory. As an alternative  
 17 implementation, the card 62 may be a storage card without processing capabilities.  
 18 In this arrangement, the storage card 62 stores the passcode or other access  
 19 credentials in a memory that is accessible by the card reader 60. During logon, the  
 20 card reader reads the passcode from the storage card 62 and compares it to the  
 21 user-supplied passcode. If there is a match, the access to the user profile and data  
 22 files on the flash memory is permitted.

23 This alternative implementation is not as secure as the smart card-based  
 24 implementation. However, it still requires user authentication and possession of  
 25



1 both components of the profile carrier during logon to gain access to the user  
2 profile and data files.

### 3 4 **Conclusion**

5 Although the invention has been described in language specific to structural  
6 features and/or methodological steps, it is to be understood that the invention  
7 defined in the appended claims is not necessarily limited to the specific features or  
8 steps described. Rather, the specific features and steps are disclosed as preferred  
9 forms of implementing the claimed invention.

10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

1 **CLAIMS**

2       **1.**     An assembly comprising:

3             a device constructed in a form factor of a PCMCIA card, the device having  
4     an interface to communicate with a storage card and memory to store user data;  
5     and

6             a removable storage card associated with a user that alternately enables  
7     access to the user data on the memory when interfaced with the device interface  
8     and disables access to the user data when removed from the device.

9  
10       **2.**     An assembly as recited in claim 1, wherein the storage card  
11     comprises a smart card.

12  
13       **3.**     An assembly as recited in claim 1, wherein the memory comprises  
14     flash memory.

15  
16       **4.**     An assembly as recited in claim 1, wherein the device stores a user's  
17     profile that can be used to configure a computer.

18  
19       **5.**     An assembly as recited in claim 1, wherein the storage card stores a  
20     passcode and access to the user data in the memory of the device is enabled upon  
21     authentication of a user-supplied passcode to the passcode stored on the storage  
22     card.

1           6.     An assembly as recited in claim 1, wherein the device stores a public  
2 key and the storage card stores a corresponding private key and access to the user  
3 data in the memory of the device is enabled upon verification that the public key  
4 and the private key are associated.

5  
6           7.     A profile carrier comprising:  
7 a storage card to store a passcode associated with a user;  
8 a PCMCIA device constructed in a form factor of a PCMCIA card, the  
9 PCMCIA device having an interface to communicate with the storage card and a  
10 memory to store a profile of the user; and

11           wherein the assembly permits access to the user profile in the memory of  
12 the PCMCIA device upon authentication of the user at the storage card via  
13 passcode verification.

14  
15           8.     A profile carrier as recited in claim 7, wherein the storage card  
16 comprises a smart card.

17  
18           9.     A profile carrier as recited in claim 7, wherein the memory comprises  
19 flash memory.

20  
21           10.    A profile carrier as recited in claim 7, wherein the PCMCIA device  
22 also stores data files.  
23  
24  
25

1           **11.**     A profile carrier as recited in claim 7, wherein the PCMCIA device  
2 stores a public key and the storage card stores a corresponding private key, and the  
3 assembly permits access to the user profile in the memory of the PCMCIA device  
4 upon verification that the public key and the private key are associated.

5  
6           **12.**     An assembly comprising:  
7           a smart card to store a passcode and a private key from a private/public key  
8 pair;  
9           a PCMCIA device constructed in a form factor of a PCMCIA card, the  
10 PCMCIA device having an interface to communicate with the smart card and flash  
11 memory to store user data and a public key from the private/public key pair;  
12           the smart card being configured to permit use of the private key following  
13 validation of a user-entered passcode with the stored passcode;  
14           the smart card being further configured to authenticate the public key stored  
15 on the memory of the PCMCIA device using the private key; and  
16           the PCMCIA device being configured to permit access to the user data  
17 stored on the memory upon successful authentication of the public key at the smart  
18 card.

19  
20           **13.**     An assembly as recited in claim 12, wherein the PCMCIA device  
21 also stores a user profile for use in configuring a computer.

22  
23           **14.**     A device comprising:  
24           a card reader constructed in a form factor of a PCMCIA card, the card  
25 reader being configured to read information from a storage card;

1 data memory resident in the card reader to store user data; and  
2 a controller resident in the card reader to enable access to the user data in  
3 the data memory in response to the card reader receiving access enabling  
4 information from a storage card.

5  
6 **15.** A device as recited in claim 14, wherein the data memory comprises  
7 flash memory.

8  
9 **16.** A device as recited in claim 14, wherein the data memory stores a  
10 user profile for use in configuring a computer.

11  
12 **17.** An assembly, comprising:  
13 the device as recited in claim 14; and  
14 a storage card that can be alternately interfaced with the card reader and  
15 removed from the card reader.

16  
17 **18.** A computer system, comprising:  
18 a computer having a PCMCIA device reader; and  
19 the assembly as recited in claim 17, wherein the assembly is interfaced with  
20 the computer via the PCMCIA device reader so that the computer can access the  
21 user data on the device.

22  
23 **19.** A PCMCIA smart card reader comprising flash memory.  
24  
25

1           **20.**     An assembly, comprising:  
2           the PCMCIA smart card reader as recited in claim 19; and  
3           a smart card that can be alternately interfaced with the smart card reader  
4           and removed from the smart card reader.

5  
6           **21.**     A computer system, comprising:  
7           a computer having a PCMCIA device reader; and  
8           the assembly as recited in claim 20, wherein the assembly is interfaced with  
9           the computer via the PCMCIA device reader.

10  
11          **22.**     A computer system, comprising:  
12          a computer having a PCMCIA device reader; and  
13          a smart card secured memory assembly having a form factor of a PCMCIA  
14          card to compatibly interface with the PCMCIA device reader in the computer, the  
15          smart card secured memory assembly having data memory to store user data and a  
16          removable smart card that alternately enables access to the user data when present  
17          and disables access to the user data when removed.

18  
19          **23.**     A computer system as recited in claim 22, wherein the data memory  
20          comprises flash memory.

21  
22          **24.**     A computer system as recited in claim 22, wherein the smart card  
23          stores a passcode and is configured to authenticate a user-supplied passcode  
24          entered into the computer as a condition for enabling access to the user data.  
25

25. A computer system as recited in claim 22, wherein:

the smart card stores a first key;

the data memory stores a second key that is associated with the first key;

and

the smart card is configured to authenticate the second key from the data memory using the first key as a condition for enabling access to the user data.

26. A computer system as recited in claim 22, wherein:

the smart card stores a passcode and a private key of a public/private key pair;

the data memory stores a public key of the public/private key pair; and

the smart card is configured to authenticate a user-supplied passcode entered into the computer as a condition for enabling access to the private key and to authenticate the public key from the data memory using the private key as a condition for enabling access to the user data.

27. A computer system, comprising:

a computer having a PCMCIA device reader;

a portable profile carrier to port a user's profile for configuration of the computer, the profile carrier having a form factor of a PCMCIA card to compatibly interface with the PCMCIA device reader in the computer, the profile carrier comprising:

(a) a storage card associated with the user;

(b) a storage card reader having an interface to communicate with the storage card and data memory to store the user's profile, the storage

1 card enabling access to the user data on the data memory of the storage  
2 card reader;

3 wherein when the profile carrier is interfaced with the computer via the  
4 PCMCIA device reader, the user's profile is accessible to configure the computer.

5  
6 **28.** A computer system as recited in claim 27, wherein the data memory  
7 comprises flash memory.

8  
9 **29.** A computer system as recited in claim 27, wherein the storage card  
10 comprises a smart card.

11  
12 **30.** A computer system as recited in claim 29, wherein the smart card  
13 stores a passcode and is configured to authenticate a user-supplied passcode  
14 entered into the computer as a condition for enabling access to the user's profile.

15  
16 **31.** A computer system as recited in claim 29, wherein:  
17 the smart card stores a first key;  
18 the storage card reader stores a second key that is associated with the first  
19 key; and

20 the smart card is configured to authenticate the second key passed in from  
21 the storage card reader using the first key as a condition for enabling access to the  
22 user's profile.



1           **32.**     A computer system as recited in claim 29, wherein:

2           the smart card stores a passcode and a private key of a public/private key  
3 pair;

4           the storage card reader stores a public key of the public/private key pair;  
5 and

6           the smart card is configured to authenticate a user-supplied passcode  
7 entered into the computer as a condition for enabling access to the private key and  
8 to authenticate the public key passed in from the storage card reader using the  
9 private key as a condition for enabling access to the user's profile.

10  
11           **33.**     A method for porting a user profile for a computer, comprising:

12           storing a user profile in data memory of a card secured profile carrier, the  
13 card secured profile carrier having a reader component with a form factor of a  
14 PCMCIA card that is equipped with the data memory and a card component that  
15 selectively enables access to the user profile in the data memory when interfaced  
16 with the reader component;

17           interfacing the card component with the reader component to form the card  
18 secured profile carrier;

19           interfacing the card secured profile carrier with the computer; and

20           reading the user profile from the data memory for use in configuring the  
21 computer.

1           **34.**    A method as recited in claim 33, further comprising interfacing the  
2 card secured profile carrier with a different second computer and reading the user  
3 profile from the data memory for use in configuring the second computer.

4  
5           **35.**    A method comprising:  
6           storing user data in a card reader;  
7           storing access credentials on a storage card, the access credentials enabling  
8 access to the user data stored on the card reader;  
9           interfacing the storage card with the card reader; and  
10          reading the access credentials from the storage card to enable access to the  
11 user data.

12  
13          **36.**    A method comprising:  
14          storing user data in memory installed in a card reader;  
15          storing a reader-resident key in the memory of the card reader;  
16          storing a card-resident key on an IC (integrated circuit) card, the card-  
17 resident key corresponding to the reader-resident key;  
18          storing a passcode on the IC card;  
19          interfacing the IC card with the card reader;  
20          receiving a user-entered passcode;  
21          permitting use of the card-resident key following validation of the user-  
22 entered passcode with the passcode stored on the IC card;  
23          passing the reader-resident key from the card reader to the IC card;  
24          authenticating, at the IC card, the reader-resident key using the card-  
25 resident key; and

1        permitting access to the user data stored in the memory of the card reader  
2 upon successful authentication of the reader-resident key.

3  
4        37.    In a system having a computer with a PCMCIA device reader and a  
5 smart card secured profile carrier having a form factor of a PCMCIA card to  
6 compatibly interface with the PCMCIA device reader in the computer, the smart  
7 card secured profile carrier having memory to store a user profile and a removable  
8 smart card, computer-readable media resident on the profile carrier having  
9 executable instructions comprising:

10        receiving a user-supplied passcode from the computer;

11        authenticating the user-supplied passcode with a passcode stored on the  
12 profile carrier;

13        enabling access to a private key on the profile carrier upon successful  
14 authentication of the user-supplied passcode;

15        authenticating a public key associated with the memory using the private  
16 key; and

17        enabling access to the user profile in the memory upon successful  
18 authentication of the public key.

1           **38.**     In a system having a computer with a PCMCIA device reader and a  
2 smart card secured profile carrier having a form factor of a PCMCIA card to  
3 compatibly interface with the PCMCIA device reader in the computer, the smart  
4 card secured profile carrier having memory to store a user profile and a removable  
5 smart card, computer-readable media at the smart card having executable  
6 instructions comprising:

7                 receiving a user-supplied passcode from the computer;

8                 authenticating the user-supplied passcode with a passcode stored on the  
9 smart card;

10                enabling access to a private key on the smart card upon successful  
11 authentication of the user-supplied passcode;

12                receiving a public key from the memory;

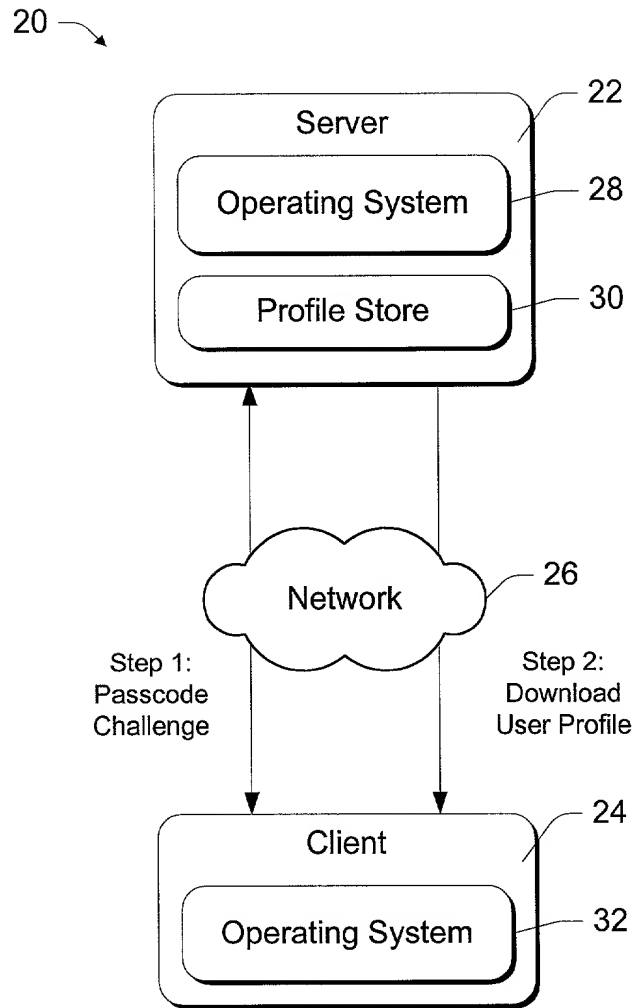
13                authenticating the public key using the private key; and

14                enabling access to the user profile in the memory of the profile carrier upon  
15 successful authentication of the public key.

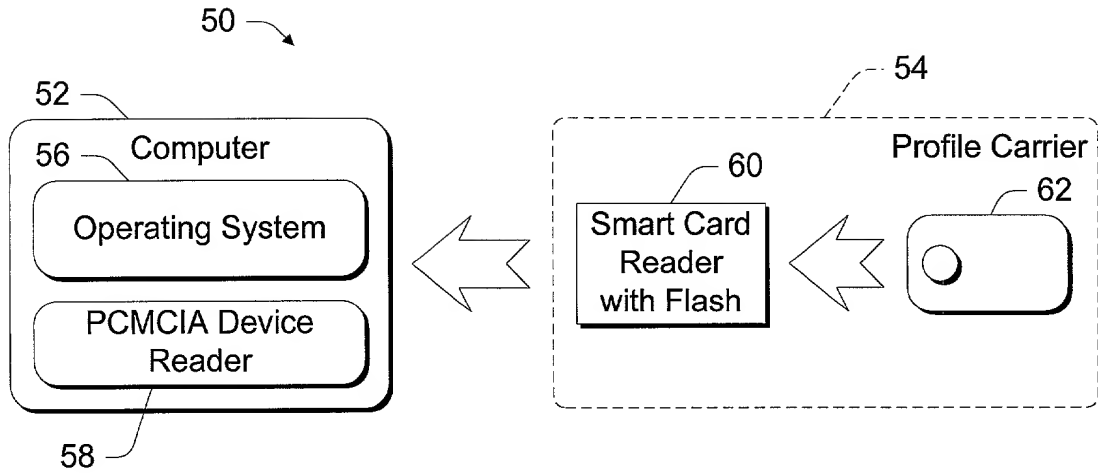
1 **ABSTRACT**

2 A portable profile carrier stores and securely transports a user's profile and  
3 data files from one computer to the next. The profile carrier is a two-component  
4 assembly comprising a smart card and a PCMCIA smart card reader. The reader is  
5 physically constructed in a form factor of a PCMCIA card and has a slot to receive  
6 the smart card. The reader has a smart card interface and controller to facilitate  
7 data communication with the smart card. The reader is equipped with data  
8 memory (e.g., flash memory) to store the user profile and data files. Access to the  
9 data memory is protected by the smart card. The composite profile carrier enables  
10 access to the user profile on the flash memory when the smart card is present and  
11 the user is authenticated, and disables access when the smart card is removed or  
12 the user is not authenticated.

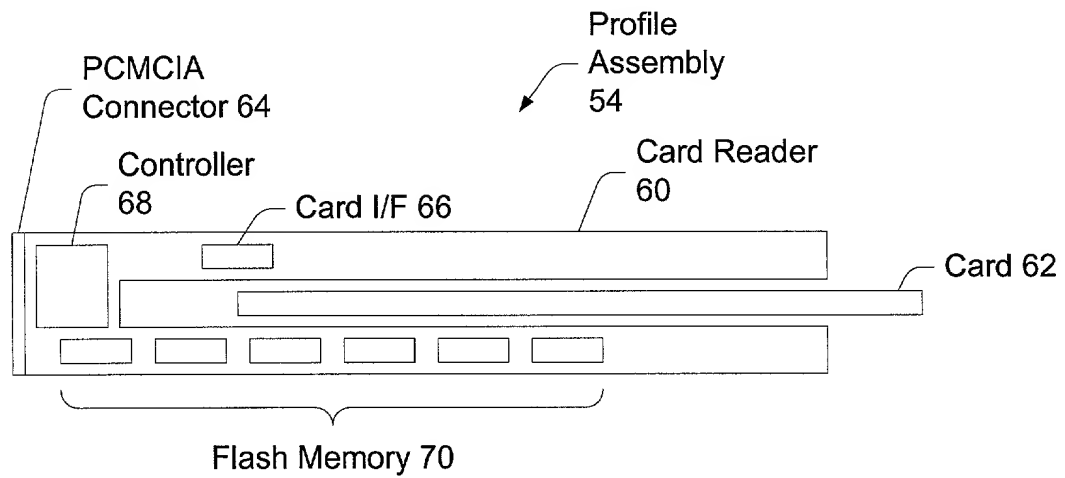
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25



*Fig. 1*  
*Prior Art*



*Fig. 2*



*Fig. 3*





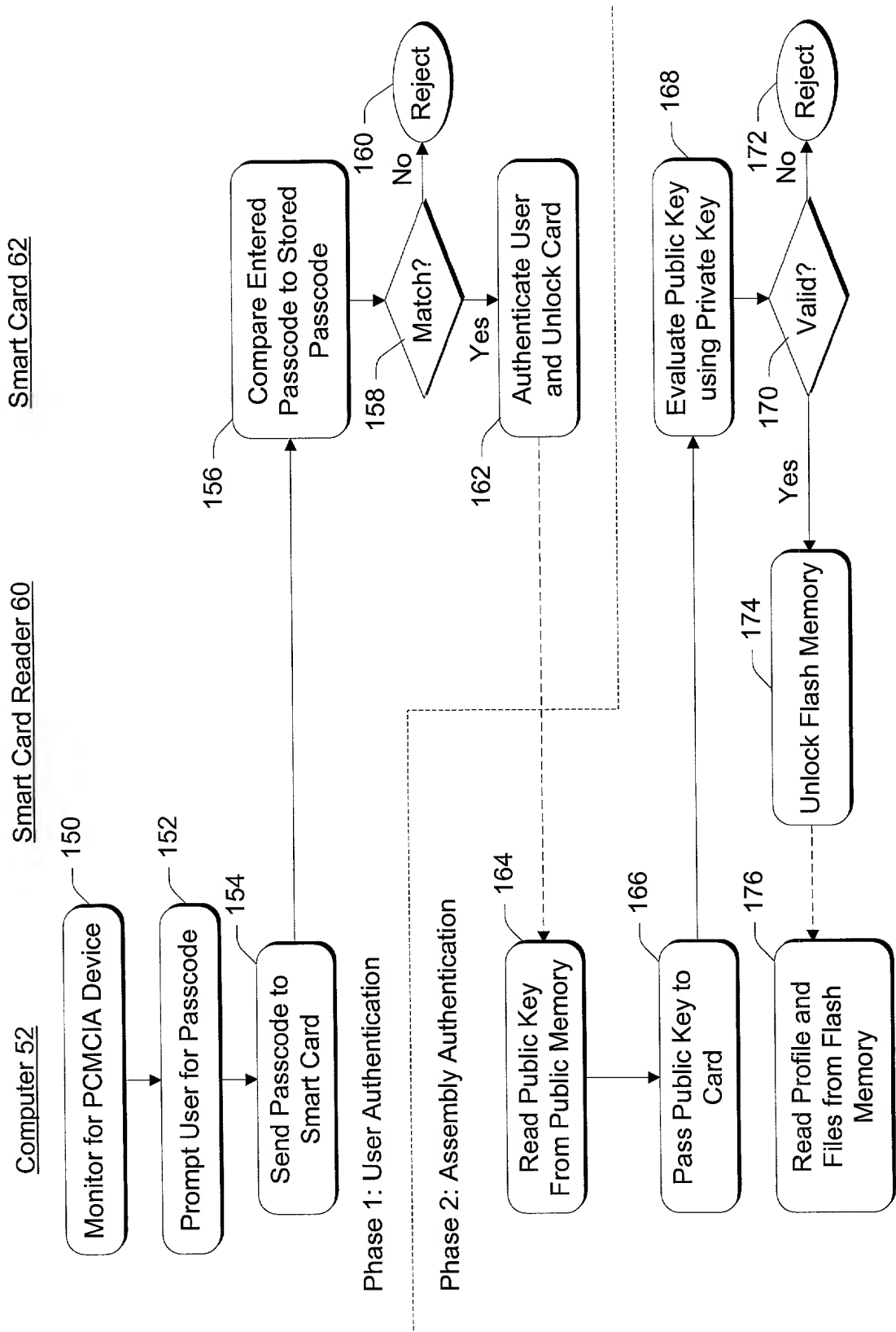


Fig. 5

1                   **IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

2   Inventorship ..... Vanzini et al.  
 3   Applicant ..... Microsoft Corporation  
 4   Attorney's Docket No. .... MS1-254US  
 5   Title: PCMCIA-compliant Smart Card Secured Memory Assembly For Porting  
       User Profiles and Documents

6                   **DECLARATION FOR PATENT APPLICATION**

7                   As a below named inventor, I hereby declare that:

8                   My residence, post office address and citizenship are as stated below next to  
 9                   my name.

10                  I believe I am the original, first and sole inventor (if only one name is listed  
 11                  below) or an original, first and joint inventor (if plural names are listed below) of the  
 12                  subject matter which is claimed and for which a patent is sought on the invention  
 13                  entitled "PCMCIA-compliant Smart Card Secured Memory Assembly For Porting  
 14                  User Profiles and Documents," the specification of which is attached hereto.

15                  I have reviewed and understand the content of the above-identified  
 16                  specification, including the claims.

17                  I acknowledge the duty to disclose information which is material to the  
 18                  examination of this application in accordance with Title 37, Code of Federal  
 19                  Regulations, § 1.56(a).

20                  PRIOR FOREIGN APPLICATIONS: no applications for foreign patents or  
 21                  inventor's certificates have been filed prior to the date of execution of this  
 22                  declaration.

23                                   **Power of Attorney**

24                  I appoint the following attorneys to prosecute this application and transact all  
 25                  future business in the Patent and Trademark Office connected with this application:  
       Lewis C. Lee, Reg. No. 34,656; Daniel L. Hayes, Reg. No. 34,618; Allan T.

Sponseller, Reg. 38,318, Steven R. Sponseller, Reg. No. 39,384, James R. Banowsky, Reg. No. 37,773, David A. Morasch, Reg. No. 42,905 Katie E. Sako, Reg. No. 32,628 and Daniel D. Crouse, Reg. No. 32,022.

Send correspondence to: LEE & HAYES, PLLC, W. 201 North River Drive, Suite 430, Spokane, Washington, 99201. Direct telephone calls to: Lewis C. Lee (509) 324-9256.

All statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statement may jeopardize the validity of the application or any patent issued therefrom.

\*\*\*\*\*

Full name of inventor: Giorgio J. Vanzini

Inventor's Signature G. Vanzini Date: 4/19/99

Residence: Seattle, WA

Citizenship: Switzerland

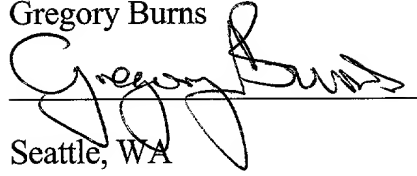
Post Office Address: 741 Boylston Ave E  
Seattle, WA 98102

\*\*\*\*\*

Full name of inventor:

Gregory Burns

Inventor's Signature



Date: 4/19/09

Residence:

Seattle, WA

Citizenship:

British

Post Office Address:

111 West Comstock Street  
Seattle, WA 98119

0324991130 MSI-254US.DE1.doc